03500.014278. PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	:	Examiner: David E. England
MASATO OCHIAI	)	
	:	TC/Art Unit: 2143
Application No.: 09/507,941	)	
	:	Confirmation No.: 2960
Filed: February 22, 2000	)	
	:	
For: NETWORK DEVICE CONTROL APPARATUS, NETWORK DEVICE CONTROL METHOD, NETWORK DEVICE CONTROL PROGRAM, AND COMPUTER-READABLE RECORDING MEDIUM STORING NETWORK CONTROL PROGRAM THEREIN	) :) :) :)	January 21, 2009

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL AND PETITION FOR EXTENSION OF TIME

Sir:

Appellant petitions to extend the time for filing an appeal brief in response to the Notice of Panel Decision from Pre-Appeal Brief Review, dated November 17, 2008, for one month, from December 17, 2008, to and including January 21, 2009 (January 17, 2009, having been a Saturday; and January 19 and 20, 2009, having been federal holidays). The extension fee of $130.00 has been paid herewith. Please charge any additional fee required for the extension, or credit any overpayment, to Deposit Account 06-1205.

The fee of $540.00 due under 37 C.F.R. §41.20(b)(2) has been paid herewith. Please charge any additional fee required in connection with the present appeal, or credit any overpayment, to Deposit Account 06-1205.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Canon Kabushiki Kaisha, Assignee of the full and exclusive right for the territory of the United States of America in and to the invention described and claimed in the present application. The Assignment was recorded in the U.S. Patent and Trademark Office on May 2, 2000, at Reel 010787, Frame 0972.

II. RELATED APPEALS AND INTERFERENCES

Appellant, Appellant's legal representative, and the Assignee are not aware of any other appeals or interferences that will directly affect, be directly affected by, or have a bearing on, the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49 are pending, of which Claims 1, 8, 9, 12, 19, 20, 47, and 49 are in independent form. Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Claims 1, 2, 4, 12, 13, 15, and 47-49 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over a document entitled "RFC 2390 - Inverse Address Resolution Protocol" (*RFC 2390*) in view of U.S. Patent No. 6,438,607 (*Fujimori et al.*). Claims 6, 9, 10, 17, 20, and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *RFC 2390* and *Fujimori et al.* in view of U.S. Patent No. 5,850,388 (*Anderson et al.*). Claims 8 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *RFC*

2390 and *Fujimori et al.* in view of U.S. Patent No. 6,310,858 (*Kano et al.*). Appellant is appealing all of the rejections of Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49.

Claims 3, 5, 7, 11, 14, 16, 18, and 22-46 have been cancelled.

The full text of each pending claim appears in the Claims Appendix, which begins on page 18.

IV. STATUS OF AMENDMENTS

A final Office Action was mailed April 17, 2008. No Amendments were filed subsequent to the mailing of the final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 is directed to a network apparatus 101 that includes a receiving unit 406 for receiving data from a network 100 (FIGS. 1-4 and 12, and page 9, lines 21-23). The network apparatus 101 also includes a detecting unit 405 for detecting a value indicative of a data length, the value being in a packet header of the data received by the receiving unit 406, and the packet header being provided for a predetermined protocol (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the network apparatus 101 includes a setting unit 405 for setting a logic address of the network apparatus 101 based on a destination logic address of the received data so that the logic address of the network apparatus and the destination logic address of the received data are the same, in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from an actual data length of the received data, and a destination physical address of the received data and

a physical address of the network apparatus 101 are the same (FIGS. 2 and 10, and page 23, line 10, through page 24, line 14).

Claim 2 depends from Claim 1 and further specifies that the setting unit 405 sets the destination logic address of the received data as the logic address of the network apparatus 101, in a case where the destination logic address of the received data and the logic address of the network apparatus 101 differ, the destination physical address of the received data and the physical address of the network apparatus 101 are the same, and the detected value indicative of the data length is the specific value (FIGS. 9 and 10, page 21, lines 11-14, and page 22, line 15, through page 24, line 14).

Claim 4 depends from Claim 1 and further specifies that the physical address is a media access control address, and that the logic address is an Internet protocol address (FIGS. 9 and 10, page 21, lines 11-14, and page 22, lines 15-23).

Claim 6 depends from Claim 1 and further specifies that the received data is an ICMP echo message by an ICMP protocol and that the detected value indicates a data length of the ICMP echo message (FIG. 9, and page 21, line 23, through page 23, line 3).

Independent Claim 8 is directed to a network apparatus 101 that includes a receiving unit 406 for receiving data from a network 100 (FIGS. 1-4 and 12, and page 9, lines 21-23). The network apparatus also includes a detecting unit 405 for detecting a TTL value, the value being in a packet header of the data received by the receiving unit 406, the packet header being provided for a predetermined protocol, and the TTL value being referred to by a router and reduced by the router when the router receives the data (FIG. 14 and page 25, lines 2-24). In addition, the network apparatus 101 includes a setting unit 304 for setting a logic address of the

network apparatus 101 based on a destination logic address of the received data so that the logic address of the network apparatus 101 and the destination logic address of the received data are the same, in a case where the detected TTL value is a specific TTL value, and a destination physical address of the received data and a physical address of the network apparatus 101 are the same. (FIG. 14 and page 25, line 25, through page 26, line 21).

Independent Claim 9 is directed to a network apparatus 101 that includes a receiving unit 406 for receiving an ICMP echo message (FIGS. 1-4 and 12, page 9, lines 21-23, and page 19, lines 5-8). The network apparatus 101 also includes a data length detecting unit 405 for detecting a value indicative of a data length, the value being in a packet header of the ICMP echo message received by the receiving unit 406 (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the network apparatus 101 includes a setting unit 405 for setting an IP address of the network apparatus 101 based on a destination IP address of the received ICMP echo message so that the IP address of the network apparatus 101 and the destination IP address of the received data are the same, if the detected value indicative of the data length is a specific value indicative of a specific data length different from an actual data length of the received ICMP echo message, and a destination MAC address of the received ICMP echo message and a MAC address of the network apparatus 101 are the same (FIGS. 9 and 10, page 21, lines 11-14, and page 22, line 15, through page 24, line 14).

Claim 10 depends from Claim 9 and further specifies that the setting unit 405 sets the IP address of the network apparatus 101 in accordance with the detected value indicative of the data length (FIG. 10, and page 23, lines 10-12).

Independent Claim 12 is directed to a method of controlling a network device 101 that includes a receiving step S1201, of receiving data from a network 100 (FIGS. 1-4 and 12, and page 9, lines 21-23). The method also includes a detecting step S1003, of detecting a value indicative of a data length, the value being in a packet header of the received data, the packet header being provided for a predetermined protocol (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the method includes a setting step S1004, of setting a logic address of the network apparatus 101 based on a destination logic address of the received data so that the logic address of the network apparatus 101 and the destination logic address of the received data are the same, in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from an actual data length of the received data, and a destination physical address of the received data and a physical address of the network apparatus 101 are the same.

Claim 13 depends from Claim 12 and further specifies that, in the setting step S1004, the destination logic address of the received data is set as the logic address of the network apparatus 101, in a case where the destination logic address of the received data and the logic address of the network apparatus 101 differ, the destination physical address of the received data and the physical address of the network apparatus 101 are the same, and the detected value indicative of the data length is the specific value (FIGS. 9 and 10, page 21, lines 11-14, and page 22, line 15, through page 24, line 14).

Claim 15 depends from Claim 4 and further specifies that the physical address is a media access control address, and that the logic address is an Internet protocol address (FIGS. 9 and 10, page 21, lines 11-14, and page 22, lines 15-23).

Claim 17 depends from Claim 15 and further specifies that the received data is an ICMP echo message by an ICMP protocol and that the detected value indicates a data length of the ICMP echo message (FIG. 9, and page 21, line 23, through page 23, line 3).

Independent Claim 19 is directed to a method of controlling a network device 101 that includes a receiving step S1201, of receiving data from a network (FIGS. 1-4 and 12, and page 9, lines 21-23). The method also includes a detecting step S1402, of detecting a TTL value, the value being in a packet header of the received data, the packet header being provided for a predetermined protocol, and the TTL value being referred to by a router and reduced by the router when the router receives the data (FIG. 14 and page 25, lines 2-24). In addition, the method includes a setting step S1404, of setting a logic address of the network apparatus 101 based on a destination logic address of the received data so that the logic addresses of the network apparatus 101 and the destination logic address of the received data are the same, in a case where the detected TTL value is a specific TTL value, and a destination physical address of the received data and a physical address of the network device 101 are the same (FIG. 14 and page 25, line 25, through page 26, line 21).

Independent Claim 20 is directed to a method of controlling a network device 101 that includes a receiving step S1201, of receiving an ICMP echo message (FIGS. 1-4 and 12, page 9, lines 21-23, and page 19, lines 5-8). The method also includes a data length detecting step S1003, of detecting a value indicative of a data length, the value being in a packet header of the received ICMP echo message (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the method includes a setting step S1004, of setting an IP address of the network apparatus 101 based on a destination IP address of the received ICMP

echo message so that the IP address of the network apparatus 101 and the destination IP address of the received data are the same, if the detected value indicative of the data length is a specific value indicative of a specific data length different from an actual data length of the received ICMP echo message, and a destination MAC address of the received ICMP echo message and a MAC address of the network device 101 are the same (FIG. 9 and 10, page 21, lines 11-14, and page 22, line 15, through page 24, line 14).

Claim 21 depends from Claim 20 and further specifies that, in the setting step S1004, the IP address of the network device 101 is set in accordance with the detected data length, if the destination IP address of the received ICMP echo message and the IP address of the network apparatus 101 differ, and the destination MAC address of the received ICMP echo message and the MAC address of the network apparatus 101 are the same (FIGS. 9 and 10, page 21, lines 11-14, page 22, line 15, through page 24, line 14).

Independent Claim 47 is directed to a network apparatus 101 that includes a receiving unit 406 and for receiving data from a network 100 (FIGS. 1-4 and 12, and page 9, lines 21-23). The network apparatus 101 also includes a detecting unit 405 for detecting a value indicative of a data length, the value being in a packet header of the data received by the receiving unit 406, and the packet header being provided for a predetermined protocol (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the network apparatus 101 also includes a setting unit 406 for setting an address of the network apparatus 101 based on a destination address of the received data so that the address of the network apparatus 101 and the destination address of the received data are the same, in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different

from an actual data length of the received data, and a destination physical address of the received data and a physical address of the network apparatus 101 are the same (FIGS. 2 and 10, and page 23, line 10, through page 24, line 14).

Claim 48 depends from Claim 47, and further specifies that the address is an Internet protocol address (FIGS. 9 and 10, page 21, lines 11-14, and page 22, lines 15-23).

Finally, independent Claim 49 is directed to a network apparatus 101 that includes a receiving unit 406 for receiving data from a network 100. The apparatus also includes a detecting unit 405 for detecting a value indicative of a data length, the value being in a packet header of the data received by the receiving unit 406, and the packet header being provided for a predetermined protocol (FIGS. 4, 9, and 10, page 22, lines 10-13, and page 22, line, 25, through page 23, line 2). In addition, the apparatus 101 includes a setting unit 405 for setting an address of the network apparatus 101 based on a first destination address of the received data so that the address of the network apparatus 101 and the first destination address of the received data are the same, in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from an actual data length of the received data, and a second destination address of the received data and an address unique to the network apparatus 101 are the same, wherein the first and second destination address differ from each other (FIGS. 2 and 10, and page 23, line 10, through page 24, line 14).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49 satisfy 35 U.S.C. § 112, first paragraph, as being supported by a written description thereof in the specification.

B. Whether Claims 1, 2, 4, 12, 13, 15, and 47-49 are patentable under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*

C. Whether Claims 6, 9, 10, 17, 20, and 21 are patentable under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*, and further in view *Anderson et al.*

D. Whether Claims 8 and 19 are patentable under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*, and further in view of *Kano et al.*

VII. ARGUMENT

A. The "Setting" Features Recited In The Claims Satisfy 35 U.S.C. § 112, First Paragraph

On pages 2-3 of the Office Action dated April 17, 2008, the Examiner alleges that, "[t]here is no teaching, in any part of the specification, that teaches the setting unit setting a logic address of a network apparatus." To support this allegation, the Examiner has cited to the following portion of the specification at page 23, lines 10-16:

> When the data length 704 is equal to 507 bytes in step S1003, the destination IP address 711 of the IP Header 502 is set as an own IP address in step S1004. After the IP address was set, the pseudo ICMP management module 405 hands the packet to the ICMP management module 404. In this instance, the unnecessary Ethernet Header and IP Header are removed.

Apparently, the Examiner interprets the cited portion of the specification as teaching that an IP address of an IP Header of a received packet is set in Step S1004, and thus the Examiner has requested that the claims be amended to state that the IP address of the IP header of the received packet is set (see page 3 of the Office Action dated April 17, 2008). For at least the following reasons, however, the Examiner's interpretation of the cited portion of the specification clearly is erroneous.

The cited portion of the specification is part of a larger discussion of FIG. 10, which illustrates a processing flow of a pseudo ICMP management module 405 (page 8, lines 16-17). The pseudo ICMP management module 405 is a component of a network protocol communication module 303 of a network board 101 (FIGS. 3 and 4, and page 11, lines 2-11). Prior to Step S1001, an IP module 406 has determined that a received packet includes an "ICMP echo request message" and has handed the received packet, including its IP Header 502, to the pseudo ICMP management module 405 (page 22, lines 6-10). In Step S1001, the pseudo ICMP management module 405 checks the Ethernet Header 501 of the received packet to determine whether a destination MAC address 601 of the received packet coincides with the network board 101's own MAC address (FIG. 10 and page 23, lines 17-20). If the destination MAC address 601 does not coincide with the network board 101's own MAC address, the packet is cancelled in Step S1106 (FIG. 10 and page 22, lines 23-24).

If the destination MAC address 601 coincides with the network board 101's own MAC address, the pseudo ICMP management module 405 determines whether a data length 704 of the IP Header 502 is equal to 509 bytes in Step S1002 (FIG. 10 and page 22, line 25, through page 23, line 2). If the data length 704 of the IP Header 502 is equal to 509 bytes, the pseudo

ICMP management module 405 sets the IP address of the network board 101 to factory-based values by setting all parameters stored in a NVRAM 205 of the network board 101 to the factory-based values (FIGS. 2 and 10, page 10, lines 13-15, page 23, lines 2-4, and page 23, line 26, through page 24, line 14).

If the data length 704 of the IP Header 502 is not equal to 509 bytes, the pseudo ICMP management module 405 determines whether the data length 704 of the IP Header 502 is equal to 507 bytes in Step S1003 (FIG. 10 and page 23, lines 6-7). If the data length 704 of the IP Header 502 is equal to 507 bytes, the pseudo ICMP management module 405 sets the IP address of the network board 101 to a destination IP address 711 of the IP Header 502 in Step S1004 (FIG. 10 and page 23, line 10, through page 24, line 11).

The Examiner's interpretation of page 23, lines 10-16, of the specification is undermined by the final sentence of the cited portion and the sentence that follows. The specification clearly discusses that, after the IP address is set in Step S1004, the pseudo ICMP management module 405 removes the Ethernet Header 501 and the IP Header 502, and hands the received packet to an ICMP management module 404 in Step S1007 (FIG. 10, and page 23, lines 13-19). The IP Header 502 of the received packet is not mentioned again in the discussion that follows the cited portion. It makes no sense to set the IP address of the IP Header 502 of the received packet, as suggested by the Examiner, and then to discard the "unnecessary" IP Header 502, which is not mentioned again, before handing the received packet over to the ICMP management module 404.

Moreover, the "Related Background Art" portion of the present application discusses that a network device can obtain an IP address from a server and set it using Dynamic

Host Configuration Protocol (DHCP), Bootstrap Protocol (BOOTP), or Reverse Address Resolution Protocol (RARP) (page 2, line 21, through page 3, line 4). Appellant submits that one skilled in the art would recognize readily that protocols such as DHCP, BOOTP, and RARP are used commonly to set IP addresses of networked devices. A discussion of several drawbacks of these protocols follows in the specification (page 3, lines 5-12). The specification goes on to state that:

> In consideration of the above drawbacks, as a method of **setting the IP address to the network device apparatus**, a method whereby there is no need to install the dedicated server to the network and the IP address is set by using a standard protocol or a standard program is demanded (page 3, lines 13-18) (emphasis added).

Based on the entire disclosure in the specification, Appellant submits that one skilled in the art would understand that, in Step S1004, the network board 101 sets its own IP address using the destination IP address of the IP Header 502 of the "ICMP echo request message" received from the PC 103, if the length of the IP Header 502 is determined to be 507 bytes in Step S1003. Therefore, the "setting" limitations presently recited in the claims are submitted to be described in the specification in such a way as to reasonablely convey to one skilled in the art that Appellant had possession of the claimed invention at the time the present application was filed.

Accordingly, reconsideration and withdrawal of the rejections of Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49 under 35 U.S.C. §112, first paragraph, are respectfully requested.

B. The Claims Are Patentable Under 35 U.S.C. § 103(a) Over The Applied Art

1. Independent Claims 1, 8, 9, 12, 19, 20, 47, and 49 are patentable over the applied art

Regarding the rejections of the independent claims under 35 U.S.C. § 103(a), the Examiner states that "[f]or Examination purposes and in light of the specification of what is truly being claimed in the Independent claims, the Examiner will treat the limitations of 'setting the apparatus address' as the 'header of the received packet as the logic address'" (see page 3 of the Office Action dated April 17, 2008). As an initial matter, Appellant notes that none of the independent claims recite "setting the apparatus address." Instead, independent Claims 1, 10, and 19 recite "setting a logic address of said network apparatus," independent Claims 8, 9, and 20 recite "setting an IP address of said network apparatus," and independent Claims 47 and 49 recite "setting an address of said network apparatus."

The specification provides a written description for "setting a logic address of said network apparatus," "setting an IP address of said network apparatus," and "setting an address of said network apparatus," as discussed in detail above. Accordingly, the independent claims should be examined based on the language presently recited in the claims.

RFC 2390 specifies an Internet standards track protocol for an Inverse Address Resolution Protocol. *RFC 2390* teaches that a station can request a protocol address corresponding to a given hardware address (Abstract). As best understood by Appellant, *RFC 2390* does not teach or suggest that the Inverse Address Resolution Protocol sets an IP address of the station.

Fujimori et al. relates to a system for implementing Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) type communications (Abstract). As best understood by Appellant, *Fujimori et al.* does not teach or suggest that an IP address of a device is set if the conditions specified in the independent claims are met.

Appellant submits that a combination of *RFC 2390* and *Fujimori et al.*, assuming such combination would even be permissible, would fail to teach or suggest a network apparatus that includes "a setting unit for setting a logic address of said network apparatus based on a destination logic address of the received data so that the logic address of said network apparatus and the destination logic address of the received data are the same in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received data, and a destination physical address of the received data and a physical address of said network apparatus are the same," as recited in Claim 1. As discussed above, the Examiner has erroneously interpreted the specification to impart a meaning to the "setting" feature that is incorrect. As such, *i.e.*, because of the erroneous interpretation, the references cited against the claims have been misapplied.

Independent Claims 8, 9, 12, 19, 20, 47, and 49 each include a "setting" feature that is similar to that of Claim 1, discussed above, in which an address of a device is set. Therefore, Claims 8, 9, 12, 19, 20, 47, and 49 also are believed to be patentable for at least the reasons discussed above.

Accordingly, reconsideration and withdrawal of the rejections of independent Claims 1, 8, 9, 12, 19, 20, 47, and 49 under 35 U.S.C. §103 are respectfully requested.

2. Dependent Claims 2, 4, 6, 10, 13, 15, 17, 21, and 48 are patentable over the applied art

Anderson et al. relates to a protocol analyzer for monitoring digital transmission networks (Abstract). As best understood by Appellant, *Anderson et al.* does not teach or suggest that the protocol analyzer disclosed therein sets an IP address of a device.

Kano et al. relates to a frame relay system that relays a received frame having a destination address and a frame TTL indicating a term of life of the received frame (Abstract). As best understood by Appellant, *Kano et al.* does not teach or suggest that the system disclosed therein sets an IP address of a device.

Nothing has been found in *Anderson et al.* and *Kano et al.* that is believed to cure the deficiencies of *RFC 2390* and *Fujimori et al.* identified above. Accordingly, reconsideration and withdrawal of the rejections of the dependent Claims 2, 4, 6, 10, 13, 15, 17, 21, and 48 under 35 U.S.C. §103 are respectfully requested.

VIII. CONCLUSION

In conclusion, Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, and 47-49 are supported by a written description thereof in the specification, in compliance with 35 U.S.C. § 112, first paragraph; Claims 1, 2, 4, 12, 13, 15, and 47-49 are not rendered obvious under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*; Claims 6, 9, 10, 17, 20, and 21 are not rendered obvious under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*, and further in view of *Anderson et al.*; Claims 8 and 19 are not rendered obvious under 35 U.S.C. § 103(a) over *RFC 2390* in view of *Fujimori et al.*, and further in view of *Kano et al.* Accordingly, the Board is respectfully requested to reverse the outstanding rejections of the claims under 35 U.S.C. § 112, first paragraph, and § 103(a).

Appellant's undersigned attorney may be reached in our New York Office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

/Lock See Yu-Jahnes/
Lock See Yu-Jahnes
Attorney for Appellant
Registration No. 38,667

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

IX. CLAIMS APPENDIX

1. (Previously Presented) A network apparatus comprising:

a receiving unit for receiving data from a network;

a detecting unit for detecting a value indicative of a data length, the value being in a packet header of the data received by said receiving unit, the packet header being provided for a predetermined protocol; and

a setting unit for setting a logic address of said network apparatus based on a destination logic address of the received data so that the logic address of said network apparatus and the destination logic address of the received data are the same in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received data, and a destination physical address of the received data and a physical address of said network apparatus are the same.

2. (Previously Presented) An apparatus according to claim 1, wherein, in a case where the destination logic address of the received data and the logic address of said network apparatus differ, the destination physical address of the received data and the physical address of said network apparatus are the same, and the detected value indicative of the data length is the specific value, said setting unit sets the destination logic address of the received data as the logic address of said network apparatus.

3. (Cancelled).

4. (Previously Presented) An apparatus according to claim 1, wherein the physical address is a media access control address, and the logic address is an Internet protocol address.

5. (Cancelled).

6. (Previously Presented) An apparatus according to claim 4, wherein the received data is an ICMP echo message by an ICMP protocol and the detected value indicates a data length of the ICMP echo message.

7. (Cancelled).

8. (Previously Presented) A network apparatus comprising:

a receiving unit for receiving data from a network;

a detecting unit for detecting a TTL value, the value being in a packet header of the data received by said receiving unit, the packet header being provided for a predetermined protocol, the TTL value being referred to by a router and reduced by the router when the router receives the data; and

a setting unit for setting a logic address of said network apparatus based on a destination logic address of the received data so that the logic address of said network apparatus and the destination logic address of the received data are the same in a case where the detected TTL value is a specific TTL value, and a destination physical address of the received data and a physical address of said network apparatus are the same.

9. (Previously Presented) A network apparatus comprising:

a receiving unit for receiving an ICMP echo message;

a data length detecting unit for detecting a value indicative of a data length, the value being in a packet header of the ICMP echo message received by said receiving unit; and

a setting unit for setting an IP address of said network apparatus based on a destination IP address of the received ICMP echo message so that the IP address of said network apparatus and the destination IP address of the received data are the same if the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received ICMP echo message, and a destination MAC address of the received ICMP echo message and a MAC address of said network apparatus are the same.

10. (Previously Presented) An apparatus according to claim 9, wherein if the destination IP address of the received ICMP echo message and the IP address of said network apparatus differ and the destination MAC address of the received ICMP echo message and the MAC address of said network apparatus are the same, said setting unit sets the IP address of said network apparatus in accordance with the detected value indicative of the data length.

11. (Cancelled).

12. (Previously Presented) A method of controlling a network device comprising:

a receiving step, of receiving data from a network;

a detecting step, of detecting a value indicative of a data length, the value being in a packet header of the received data, the packet header being provided for a predetermined protocol; and

a setting step, of setting a logic address of said network apparatus based on a destination logic address of the received data so that the logic address of said network apparatus and the destination logic address of the received data are the same in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received data, and a destination physical address of the received data and a physical address of the network device are the same.

13. (Previously Presented) A method according to claim 12, wherein, in a case where the destination logic address of the received data and the logic address of said network apparatus differ, the destination physical address of the received data and the physical address of said network apparatus are the same, and the detected value indicative of the data length is the specific value, said setting step sets the destination logic address of the received data as the logic address of said network apparatus.

14. (Cancelled).

15. (Previously Presented) An apparatus according to claim 4, wherein the received data is an ICMP echo message by an ICMP protocol and the detected value indicates a data length of the ICMP echo message.

16. (Cancelled).

17. (Previously Presented) A method according to claim 15, wherein the received data is an ICMP echo message by an ICMP protocol and the detected value indicates a data length of the ICMP echo message.

18. (Cancelled).

19. (Previously Presented) A method of controlling a network device comprising:

a receiving step, of receiving data from a network;

a detecting step, of detecting a TTL value, the value being in a packet header of the received data, the packet header being provided for a predetermined protocol, the TTL value being referred to by a router and reduced by the router when the router receives the data; and

a setting step, of setting a logic address of said network apparatus based on a destination logic address of the received data so that the logic addresses of said network apparatus and the destination logic address of the received data are the same in a case where the detected TTL value is a specific TTL value, and a destination physical address of the received data and a physical address of the network device are the same.

20. (Previously Presented) A method of controlling a network device comprising:

a receiving step, of receiving an ICMP echo message;

a data length detecting step, of detecting a value indicative of a data length, the value being in a packet header of the received ICMP echo message; and

a setting step, of setting an IP address of said network apparatus based on a destination IP address of the received ICMP echo message so that the IP address of said network apparatus and the destination IP address of the received data are the same if the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received ICMP echo message, and a destination MAC address of the received ICMP echo message and a MAC address of the network device are the same.

21. (Preciously Presented) A method according to claim 20, wherein in said setting step, if the destination IP address of the received ICMP echo message and the IP address of said network apparatus differ and the destination MAC address of the received ICMP echo message and the MAC address of said network apparatus are the same, the IP address of the network device is set in accordance with the detected data length.

22. - 46. (Cancelled).

47. (Previously Presented) A network apparatus comprising:

a receiving unit for receiving data from a network;

a detecting unit for detecting a value indicative of a data length, the value being in a packet header of the data received by said receiving unit, the packet header being provided for a predetermined protocol; and

a setting unit for setting an address of said network apparatus based on a destination address of the received data so that the address of said network apparatus and the destination address of the received data are the same in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received data, and a destination physical address of the received data and a physical address of said network apparatus are the same.

48. (Previously Presented) An apparatus according to claim 47, wherein the address is an Internet protocol address.

49. (Previously Presented) A network apparatus comprising:

a receiving unit for receiving data from a network;

a detecting unit for detecting a value indicative of a data length, the value being in a packet header of the data received by said receiving unit, the packet header being provided for a predetermined protocol; and

a setting unit for setting an address of said network apparatus based on a first destination address of the received data so that the address of said network apparatus and the first destination address of the received data are the same in a case where the detected value indicative of the data length is a specific value indicative of a specific data length different from actual data length of the received data, and a second destination address of the received data and an address unique to said network apparatus are the same,

wherein the first and second destination address differ from each other.

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS APPENDIX

None

FCHS_WS 2783051v2